



## On the additive theory of prime numbers II

Patrick Cegielski, Denis Richard, Maxim Vsemirnov

### ► To cite this version:

Patrick Cegielski, Denis Richard, Maxim Vsemirnov. On the additive theory of prime numbers II. 2005, pp.39-47. hal-00096769

**HAL Id: hal-00096769**

**<https://hal.science/hal-00096769>**

Submitted on 20 Sep 2006

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# On the additive theory of prime numbers II

Patrick CEGIELSKI<sup>‡</sup> Denis RICHARD<sup>§</sup> & Maxim VSEMIRNOV<sup>¶</sup>

September 20, 2006

## Abstract

The undecidability of the additive theory of primes (with identity) as well as the theory  $\text{Th}(\mathbb{N}, +, n \mapsto p_n)$ , where  $p_n$  denotes the  $(n+1)$ -th prime, are open questions. As a possible approach, we extend the latter theory by adding some extra function. In this direction we show the undecidability of the existential part of the theory  $\text{Th}(\mathbb{N}, +, n \mapsto p_n, n \mapsto r_n)$ , where  $r_n$  is the remainder of  $p_n$  divided by  $n$  in the euclidian division.

## Résumé

L'indécidabilité de la théorie additive des nombres premiers ainsi que de la théorie  $\text{Th}(\mathbb{N}, +, n \mapsto p_n)$ , où  $p_n$  désigne le  $(n+1)$ -ième premier, sont deux questions ouvertes. Nous étendons cette dernière théorie en lui ajoutant une fonction supplémentaire et nous montrons l'indécidabilité de la théorie  $\text{Th}(\mathbb{N}, +, n \mapsto p_n, n \mapsto r_n)$ , où  $r_n$  désigne le reste de  $p_n$  de la division euclidienne de  $p_n$  par  $n$ , et même de sa seule partie existentielle.

**Introduction** - The additive theory of primes contains longtime open classical conjectures of Number Theory, as famous GOLDBACH's binary conjecture or TWIN PRIMES conjecture, and so on. Some authors provided [BJW,BM,LM] conditional proofs (through SCHINZEL's Hypothesis [SS]) of the undecidability of the additive theory of primes  $\text{Th}(\mathbb{N}, +, \mathbb{P})$ , where  $\mathbb{P}$  is the set of all primes. Weakening the problem by strengthening this theory, we introduced [CRV] the theory  $\text{Th}(\mathbb{N}, +, n \mapsto p_n)$ , where  $p_n$  is the  $(n+1)$ -th prime, and posed the problem of its (un)decidability. As usual for a language containing a function symbol, we suppose it contains identity. Note that  $\mathbb{P}$  is existentially definable within  $\langle \mathbb{N}, n \mapsto p_n \rangle$ , hence  $\text{Th}(\mathbb{N}, +, \mathbb{P})$  is a subtheory of  $\text{Th}(\mathbb{N}, +, n \mapsto p_n)$ . At the moment, the undecidability of the latter theory is still an open question, and our approach in [CRV] was to consider several approximations of the function  $n \mapsto p_n$  as, for instance,  $n \lfloor \log n \rfloor$  and on this way we showed the undecidability of theories  $\text{Th}(\mathbb{N}, +, nf(n))$  for a family of functions  $f$  including  $\lfloor \log \rfloor$  mentioned above. Another approach consists of extending the language  $\{+, n \mapsto p_n\}$  to  $\{+, n \mapsto p_n, n \mapsto r_n\}$ , where  $r_n$  is the remainder of  $p_n$  divided by  $n$ . The main result of this paper is the following:

**Theorem 1** *Multiplication is existentially  $\langle \mathbb{N}, +, n \mapsto p_n, n \mapsto r_n \rangle$ -definable at first-order.*

This leads to the following (without use of conjectures) result:

---

<sup>‡</sup>LACL, UMR-FRE 2673, Université Paris 12, IUT Route Forestière Hurtault F-77300 Fontainebleau,  
- Email: cegielski@univ-paris12.fr

<sup>§</sup>LLAIC1 Université d'Auvergne, IUT Informatique, B.P. 86, F-63172 Aubière Cedex  
- Email: richard@iut.u-clermont1.fr

<sup>¶</sup>Steklov Institute of Mathematics (POMI), 27 Fontanka St Petersburg, 191011, Russia  
- Email: vsemir@pdmi.ras.ru

**Corollary 1**  $\text{Th}_{\exists}(\mathbb{N}, +, n \mapsto p_n, n \mapsto r_n)$  is undecidable.

Remark Actually all positive integer constants are existentially  $\{+, \mathbb{P}\}$ -definable in the following manner:

$$\begin{aligned} x = 0 & \Leftrightarrow x + x = x; \\ x = 1 & \Leftrightarrow \exists y(y = x + x \wedge y \in \mathbb{P}); \\ x = 2 & \Leftrightarrow \exists y(y = 1 \wedge x = y + y); \\ & \vdots \\ x = n + 1 & \Leftrightarrow \exists y \exists z(y = n \wedge z = 1 \wedge x = y + z). \end{aligned}$$

As we mentioned above,  $\mathbb{P}$  is existentially definable within the language  $\{+, n \mapsto p_n\}$ , hence all positive integer constants are also existentially  $\{+, n \mapsto p_n\}$ -definable. Note, that  $n \lfloor \frac{p_n}{n} \rfloor = p_n - r_n$ . We intend to define (section 2, see Lemma 3)  $\lfloor \frac{p_n}{n} \rfloor$  from  $+$  and  $n \lfloor \frac{p_n}{n} \rfloor$ . Then the strategy will be to define multiplication through the function  $n \mapsto cn^2$  (where  $c$  is a fixed constant), which is to be proved  $\{+, \lfloor \frac{p_n}{n} \rfloor, n \lfloor \frac{p_n}{n} \rfloor\}$ -definable. Consequently, multiplication will be existentially  $\{+, n \mapsto p_n, n \mapsto r_n\}$ -definable at first-order.

Remark. In the previous paper [CRV] we consider continuous real strictly increasing functions and their inverses. Since we work with integer parts we have to introduce pseudo-inverses of discrete functions. For such a discrete unbounded function  $f$  from  $\mathbb{N}$  into  $\mathbb{N}$ , we define its pseudo-inverse  $f^{-1}$  from  $\mathbb{N}$  into  $\mathbb{N}$  by  $f^{-1}(n) = \mu m[f(m+1) > n]$ , where  $\mu$  means “the smallest ... such that”. Due to the unboundness of  $f$  such an  $f^{-1}$  is correctly defined.

## 1) Some preliminary results in Number Theory

Contrarily to what happens with  $\log$ , the behavior of  $\lfloor \frac{p_n}{n} \rfloor$  is *a priori* irregular but we shall prove it is not too much chaotic. Namely, we prove:

**Proposition 1** Let us denote the mapping  $n \mapsto \lfloor \frac{p_n}{n} \rfloor$  by  $f$ .

- 1) For  $m > n$ , we have  $f(m) - f(n) \geq -1$ ;
- 2) For  $n \geq 11$ , we have  $f^{-1}(n+1) - f^{-1}(n) > n$ .

**Proof** 1) We use the following estimates for  $p_n$  ([RP], p. 249):

$$\begin{aligned} p_m &\geq m \log m + m \log \log m - 1.0072629m \quad \text{for } m \geq 2; \\ p_m &\leq m \log m + m \log \log m - 0.9385m \quad \text{for } m \geq 7022. \end{aligned} \tag{1}$$

For  $m > n \geq 7022$ , we have  $f(m) - f(n) = \lfloor \frac{p_m}{m} \rfloor - \lfloor \frac{p_n}{n} \rfloor$   
 $\geq \frac{p_m}{m} - \frac{p_n}{n} - 1 \geq \log(\frac{m}{n}) - \log(\frac{\log m}{\log n}) - 0.9385 + 1.0072629 - 1$ .

Hence  $f(m) - f(n) \geq -1$  because the sum of the two first terms is positive as is the sum of terms three and four.

If  $n < 7022$ , one may check the desired inequality by a direct computation.

2) Let  $m$  be  $f^{-1}(n)$ . By the very definition of  $f^{-1}$ , the equality  $m = f^{-1}(n)$  is equivalent to the conjunction of the two following conditions:

$$\left\{ \begin{array}{l} \left\lfloor \frac{p_{m+1}}{m+1} \right\rfloor \geq n+1; \\ \forall k \leq m \quad \left\lfloor \frac{p_k}{k} \right\rfloor \leq n. \end{array} \right. \tag{2}$$

For  $k \leq 7022$ , the maximum of  $\frac{p_k}{k}$  is attained for  $k = 7012$  and equal to  $\frac{p_{7012}}{7012} < 10.102824 < 11$ . Consequently, we see that  $m = f^{-1}(n) \geq f^{-1}(11) \geq 7022$  and this is the reason why in the hypothesis of Proposition 1, item 2) we assume  $n \geq 11$ .

To prove the inequality, it is sufficient to prove that for  $k = m + n$  we have  $\lfloor \frac{p_k}{k} \rfloor \leq n + 1$ , or in other words,

$$\frac{p_k}{k} < n + 2. \quad (3)$$

Note that for  $m \geq 7022$ , we have by (2):

$$n + 1 \leq \left\lfloor \frac{p_{m+1}}{m+1} \right\rfloor + 1 \leq \frac{p_{m+1}}{m+1} + 1 \leq \log(m+1) + \log \log(m+1) - 0.07 < m.$$

Consequently it is sufficient – and actually more convenient – to prove a somehow stronger result, namely the same inequality (3) but for  $m \geq 7022$  and  $m + 1 \leq k \leq 2m$ .

From the second estimate of (1) we have, since  $k \geq m \geq 7022$ , the following inequalities:

$$\begin{aligned} \frac{p_k}{k} &< \log k + \log \log k - 0.9385 \\ &\leq \log 2m + \log \log 2m - 0.9385 \\ &= \log m + \log \log m + \log 2 + \log(1 + \frac{\log 2}{\log m}) - 0.9385; \end{aligned}$$

using the first estimate of (1) and  $\frac{\log 2}{\log m} \leq \frac{\log 2}{\log 7022}$ , we have:

$$\log m + \log \log m - 1.0072629 \leq \frac{p_m}{m};$$

consequently:

$$\frac{p_k}{k} \leq \frac{p_m}{m} + 0.07 + \log 2 + \log(1 + \frac{\log 2}{\log 7022}) \leq \frac{p_m}{m} + 1$$

by an easy computation and finally, due to (2), we obtain  $\frac{p_k}{k} < n + 2$ .  $\square$

Item 1) of previous proposition emphasizes on the fact that  $f : n \mapsto \lfloor \frac{p_n}{n} \rfloor$  is “almost” increasing and item 2) shows that the difference  $f^{-1}(n+1) - f^{-1}(n)$  is big enough with respect to  $n$ . This suggests to introduce a new class of functions, containing  $f$ , for which we prove that the existential part of the theory  $\text{Th}(\mathbb{N}, +, n \mapsto nf(n))$  is undecidable.

## 2) The class $C(k, d, n_0)$ and some its properties

### 2.1) The class $C(k, d, n_0)$

Let  $k \geq 0$  be a fixed nonnegative integer. We shall say  $f$  is *k-almost increasing* if and only if

$$\forall y \geq x [f(y) - f(x) \geq -k]. \quad (4)$$

In this sense 0-almost increasing means increasing (not necessarily strictly) and  $n \mapsto \lfloor \frac{p_n}{n} \rfloor$  is 1-almost increasing (due to Proposition 1).

Still looking at  $n \mapsto \lfloor \frac{p_n}{n} \rfloor$ , we intend to consider functions whose pseudo-inverse is defined and asymptotically increases quickly enough with respect to its argument. Let us say that  $f^{-1}$  has at least  $(1/d)$ -linear difference, if

$$\exists n_0 \in \mathbb{N} \forall n \geq n_0 [f^{-1}(n+1) - f^{-1}(n) > \frac{n}{d}]. \quad (5)$$

In fact, for  $\lfloor \frac{p_n}{n} \rfloor$ , the constant  $d$  is 1 and  $n_0 = 11$ , but results and proofs hold for an arbitrary (fixed)  $d$ .

Now let us define the class  $C(k, d, n_0)$  as the set of functions from  $\mathbb{N}$  into  $\mathbb{N}$  satisfying conditions (4) of being *k-almost increasing* and (5) of having its pseudo-inverse with an *at least  $(1/d)$ -linear difference*.

In order to prove FUNDAMENTAL LEMMA of section 3, whose Theorem 1 is a corollary, we show some properties of the class  $C(k, d, n_0)$ . Firstly, in section 2.2 we present in three lemmas these properties and comment them. Afterwards, in section 2.3, we prove them.

## 2.2) Properties of $C(k, d, n_0)$

**Lemma 1** *For any function  $f \in C(k, d, n_0)$  the following items hold:*

- (i) *For any  $n \geq n_0$ , we have  $f^{-1}(n + d) - f^{-1}(n) > n$ ;*
- (ii) *For any  $n \geq n_0 + 1$ , the set  $\{x \in \mathbb{N} \mid f(x) = n\}$  is nonempty;*
- (iii) *For any  $n \geq n_0 + 1$ , the equality  $f(x) = n$  implies*

$$x > \frac{1}{2d}[(n-1)(n-2) - n_0(n_0-1)].$$

**Lemma 2** *If  $f \in C(k, d, n_0)$  and  $f(x) = n \geq n_0$ , then for any  $c$  such that  $1 \leq c \leq n$ , we have:*

$$-k \leq f(x + c) - f(x) \leq k + d. \quad (6)$$

**Lemma 3** *For any  $f \in C(k, d, n_0)$ , let  $x_0 = f^{-1}(2 + 4d + n_0^2 + k)$ .*

*Consider  $\tilde{f} : [x_0 + 1, +\infty[ \cap \mathbb{N} \longrightarrow \mathbb{N}$  with  $\tilde{f}(x) = f(x)$ . Then  $\tilde{f}$  is existentially definable at first-order within  $\langle \mathbb{N}, +, 1, x \mapsto xf(x) \rangle$ .*

Remarks 1) Item (i) of Lemma 1 provides a linear lower bound of values of  $f^{-1}$  when difference of arguments is the parameter  $d$  of the considered class.

Item (ii) of the same lemma insure that  $f$  is asymptotically onto, and item (iii) gives a quadratic lower bound for solutions of the equation  $f(x) = n$ , that we need in section 3.

2) Actually, as the reader will see within the proof, Lemma 1 does not use condition (4) of being *k-almost increasing*.

3) Lemma 2 provides asymptotical bounds for the difference of two values of  $f$  with arguments taken in a short interval with respect to the values of these arguments. Referring to the previous Lemma 1 we see that  $n$  is at most  $\sqrt{2dx + n_0^2} + 2$ .

4) Lemma 3 generalizes the situation of the main result of the previous paper [CRV] of the same authors when  $\lfloor \log n \rfloor$  was “extracted”, *i.e.* defined, from  $+$  and  $n \lfloor \log n \rfloor$ .

## 2.3) Proofs of the three Lemmas

**Proof of Lemma 1** (i) By condition (5):

$$\begin{aligned} f^{-1}(n + d) - f^{-1}(n) &= [f^{-1}(n + d) - f^{-1}(n + d - 1)] \\ &\quad + [f^{-1}(n + d - 1) - f^{-1}(n + d - 2)] \\ &\quad + \dots \\ &\quad + [f^{-1}(n + 1) - f^{-1}(n)] \\ &> \frac{n+d-1}{d} + \frac{n+d-2}{d} + \dots + \frac{n}{d} \\ &> n. \end{aligned} \quad 4$$

(ii) If there was no  $x$  such that  $f(x) = n$ , we would have  $f^{-1}(n) = f^{-1}(n-1)$ . But  $f^{-1}(n) > f^{-1}(n-1)$  according to condition (5).

(iii) By definition of  $f^{-1}$ , we have:  $x > f^{-1}(n-1)$ .

As in (i), we have:

$$\begin{aligned} f^{-1}(n-1) - f^{-1}(n_0) &= [f^{-1}(n-1) - f^{-1}(n-2)] \\ &\quad + \dots \\ &\quad + [f^{-1}(n_0+1) - f^{-1}(n_0)] \\ &> \frac{n-2}{d} + \frac{n_0}{d} + \dots + \frac{n}{d} \\ &= \frac{(n-2)(n-1) - n_0(n_0+1)}{2d}. \end{aligned}$$

and the result.  $\square$

**Proof of Lemma 2** The left-hand side of the inequality is an immediate consequence of the very definition of a  $k$ -almost increasing function. For proving the right-hand side, note that, using  $k$ -almost increasing property of  $f$  together with  $f(x) = n$ , we obtain:

$$\max_{y \leq x} f(y) \leq f(x) + k = n + k,$$

so that  $f^{-1}(n+k) \geq x$ , by the definition of  $f^{-1}$ . By previous Lemma 1, item (i) and the latter inequality, we have:

$$f^{-1}(n+k+d) > f^{-1}(n+k) + n+k \geq x+n+k \geq x+n \geq x+c$$

since  $1 \leq c \leq n$ . Using again the definition of  $f^{-1}$ , we see that  $f(x+c) \leq n+k+d = f(x) + k+d$  and we are done.  $\square$

**Proof of Lemma 3** To define  $\tilde{f}$  within the structure  $\langle \mathbb{N}, +, x \mapsto xf(x) \rangle$  we shall make use of the inequality:

$$0 \leq f(x) < x$$

together with the remainder of  $f(x)$  modulo  $x+1$ , which we must define in the considered structure.

**Fact 1.-**  $f(x) < x$ .

By the definition of  $f^{-1}$ , we have  $f(x_0+1) > k+2+4d+n_0^2$  and by the  $k$ -almost increasing property we deduce, for  $x \geq x_0+1$ ,

$$n = f(x) \geq f(x_0+1) - k > 2 + 4d + n_0^2. \quad (7)$$

Hence  $\frac{n-2}{2d} > 2$ .

From (7), we obtain  $n > n_0+1$  so that by Lemma 1, item (iii), we have:

$$x > \frac{1}{2d}[(n-1)(n-2) - n_0(n_0-1)],$$

hence:

$$x > 2(n-1) - \frac{n_0(n_0-1)}{2d} > 2(n-1) - n_0^2 = n + (n-2-n_0^2) > n = f(x). \quad \square \square$$

**Fact2.-** We have:

$$f(x) \equiv (x+1)f(x+1) - xf(x) \pmod{x+1}. \quad (8)$$

It is sufficient to note that  $(x+1)f(x+1) - xf(x) = f(x) + (x+1)[f(x+1) - f(x)]$ .  $\square\square$

We are still unable to define general congruences, fortunately here the difference  $|f(x+1) - f(x)|$  is bounded, namely,

$$|f(x+1) - f(x)| \leq k + d, \quad (9)$$

due to Lemme 2, with  $c = 1$ . This suggests to introduce the notion of a restricted congruence, namely, for  $a, b, m$  in  $\mathbb{N}$  and some fixed integer  $c$ , we define  $a \equiv_c b \pmod{m}$  by:

$$\bigvee_{h=0}^c \{[a = b + \underbrace{m + \dots + m}_{h \text{ times}}] \vee [b = a + \underbrace{m + \dots + m}_{h \text{ times}}]\}.$$

Obviously, the first-order latter formula is expressible within the structure  $\langle \mathbb{N}, + \rangle$ , since  $c$  is fixed. The congruence (8) and inequality (9) provide together the following restricted congruence:

$$f(x) \equiv_{k+d} (x+1)f(x+1) - xf(x) \pmod{x+1},$$

which is a definition of  $f(x)$  within  $\langle \mathbb{N}, +, 1, x \mapsto xf(x) \rangle$  since  $1 \leq f(x) < x$ . Finally, we provide explicitly an existential first-order definition of  $f$ , namely:

$$[x > x_0 \wedge y = f(x)] \leftrightarrow$$

$$\begin{aligned} \{x > x_0 \wedge y \leq x \wedge \bigvee_{h=0}^{k+d} [(y + xf(x) = (x+1)f(x+1) + \underbrace{(x+1) + \dots + (x+1)}_{h \text{ times}}) \\ \vee ((x+1)f(x+1) = y + xf(x) + \underbrace{(x+1) + \dots + (x+1)}_{h \text{ times}})]\}. \end{aligned}$$

### 3) Fundamental Lemma and the proof of the Main Theorem

In order to prove the undecidability of  $\text{Th}(\mathbb{N}, n \mapsto p_n, n \mapsto r_n)$ , we prove a more general result, namely:

**Lemma 4 (Fundamental Lemma)** *For any  $f \in C(k, d, n_0)$  [see §2], multiplication is existentially  $\{+, 1, x \mapsto xf(x)\}$ -definable at first-order.*

As shown by Y. MATIYASEVICH, the existential true theory of numbers is exactly the set of arithmetical relations, which are definable by diophantine equations. Therefore the negative solution of the 10-th Hilbert's problem [MY] implies the following corollary.

**Corollary 2** *The existential theory  $\text{Th}_{\exists}(\mathbb{N}, +, 1, x \mapsto xf(x))$  is undecidable.*

**Proof of Lemma 4** It suffices to show that for some constants  $c$  and  $n_1$  the function  $n \mapsto cn^2$  from  $[n_1, +\infty[ \cap \mathbb{N}$  into  $\mathbb{N}$  is  $\{+, 1, x \mapsto xf(x)\}$ -definable. More precisely, we shall take  $c = 5d$  and  $n_1 = 2 + 5d + n_0^2$ . Consider  $n \geq n_1$ . Since  $n_1 > n_0 + 1$ , we can apply Lemma 1, item (ii), proving there exists  $x$  such that  $f(x) = 5dn$ . Let  $x_0$  be the same as in Lemma 3, namely  $x_0 = f^{-1}(2 + 4d + n_0^2 + k)$ . Let us show  $x > x_0$ . Otherwise  $x \leq x_0$ , so that by the  $k$ -almost increasing property  $f(x) \leq f(x_0) - k$ , implying, by the definitions of  $f^{-1}$  and  $x_0$ ,

$$f(x) \leq 2 + 4d + n_0^2 + k - k \underset{6}{<} n_1 < 5dn_1 \leq 5dn = f(x),$$

which is impossible.

Note that  $5dn$  is  $\{+\}$ -definable as the sum of  $5d$  terms equal to  $n$  ( $d$  is a fixed constant).

Now thanks to Lemma 3, an  $x$  such that  $f(x) = 5dn$  is  $\{+, 1, x \mapsto xf(x)\}$ -definable.

On the other hand:

$$(x+n)f(x+n) - xf(x) = (x+n)[f(x+n) - f(x)] + nf(x) = (x+n)[f(x+n) - f(x)] + 5dn^2.$$

By Lemma 2 applied to  $c = n$ , we have  $|f(x+n) - f(x)| \leq k + d$ , so that:

$$5dn^2 \equiv_{k+d} (x+n)f(x+n) - xf(x) \pmod{x+n}. \quad (10)$$

According to Lemma 1 and item (iii) since  $f(x) = 5dn$  and  $5dn > n_1 > n_0 + 1$  the inequalities  $n \geq n_1 > n_0^2$  and:

$$\begin{aligned} x+n &> \frac{(5dn-1)(5dn-2)}{2d} - \frac{n_0(n_0-1)}{2d} + n \\ &> \frac{25d^2n^2 - 15nd}{2d} > 5dn^2 \end{aligned} \quad (11)$$

hold.

Using (10) and (11), a similar argument as in Lemma 3 shows that the function  $n \mapsto 5dn^2 = cn^2$  with domain  $[n_1, +\infty[ \cap \mathbb{N}$  is existentially  $\{+, 1, x \mapsto xf(x)\}$ -definable. By a routine argument, multiplication is clearly existentially  $\{+, 1, x \mapsto xf(x)\}$ -definable.  $\square$

**Proof of the Main-Theorem** We remind the reader that 1 was existentially  $\{+, \mathbb{P}\}$  and  $\{+, n \mapsto p_n\}$ -defined in the introduction.

We also noted that  $n \lfloor \frac{p_n}{n} \rfloor = p_n - r_n$  and  $n \mapsto n \lfloor \frac{p_n}{n} \rfloor$  belongs to  $C(1, 1, 11)$ , the latter due to Proposition 1, §1. Then Fundamental Lemma can be applied and multiplication is existentially  $\{+, n \mapsto p_n, n \mapsto r_n\}$ -definable.  $\square$

**Conclusion:** Our main result is absolute in the sense that does not depend on any conjecture. In order to shed more light on the considered theories  $\text{Th}_{\exists}(\mathbb{N}, +, \mathbb{P})$  and  $\text{Th}_{\exists}(\mathbb{N}, n \mapsto p_n, n \mapsto r_n)$ , we recall a conditional result of A. WOODS. Let us recall that DICKSON'S CONJECTURE [DL] claims that if  $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$  are integers with all  $a_i > 0$  and

$$\forall y \neq 1 \exists x [y \nmid \prod_{1 \leq i \leq n} (a_i x + b_i)]$$

then there exist infinitely many  $x$  such that  $a_i x + b_i$  are primes for all  $i$ . Let us call *DC* this conjecture, then A. WOODS proved [WA]:

*If DC is true then the existential theory  $\text{Th}_{\exists}(\mathbb{N}, +, \mathbb{P})$  is decidable.*

Now, the question is to know whether there is a gap between  $\text{Th}_{\exists}(\mathbb{N}, +, n \mapsto p_n, n \mapsto r_n)$  or whether they are exactly the same. In the case of equality between these two theories, *DC* is false (and hence SCHINZEL'S HYPOTHESIS on primes, whose *DC* is the linear case, is also false).

**Open problem:** *Is  $\text{Th}_{\exists}(\mathbb{N}, +, \mathbb{P})$  equal to  $\text{Th}_{\exists}(\mathbb{N}, +, n \mapsto p_n, n \mapsto r_n)$ ?*

## References

[BJW] P.T. BATEMAN, C.G. JOCKUSCH and A.R. WOODS, *Decidability and Undecidability of theories with a predicate for the prime*, **Journal of Symbolic Logic**, vol. 58, 1993, pp.672-687.



- [BM] Maurice BOFFA, *More on an undecidability result of BATEMAN, JOCKUSCH and WOODS*, **Journal of Symbolic Logic**, vol. 63, 1998, p.50.
- [CRV] Patrick CEGIELSKI, Denis RICHARD & Maxim VSEMIRNOV, *On the additive Theory of Prime Numbers I*, **Proceedings of CSIT'2003** (Computer Science and Information Technologies), September 22-26, 2003, Yerevan, Armenia, 459 p., pp. 80–85.
- [DL] L.E. DICKSON, *A new extension of DIRICHLET's theorem on prime numbers*, **Messenger of Mathematics**, vol. 33 (1903–04), pp. 155–161.
- [LM] T. LAVENDHOMME & A. MAES, *Note on the undecidability of  $\langle \omega, +, P_{m,r} \rangle$* , Definability in arithmetics and computability, 61-68. **Cahier du Centre de logique**, Belgium, 11 (2000).
- [MY] Yuri MATIYASEVICH, **Hilbert's tenth Problem**, The MIT Press, Foundations of computing, 1993, XXII+262p.
- [RP] Paul RIBENBOIM, **The new book of Prime records**, Springer, 1996, XIV+541p.
- [SS] A. SCHINZEL & W. SIERPIEŃSKY, *Sur certaines hypotheses concernant les nombres premiers*, **Acta Arithmetica**, vol. 4, 1958, 185–208 and 5, 1959, 259.
- [WA] Alan WOODS, **Some problems in logic and number theory, and their connection**, Ph.D. thesis, University of Manchester, Manchester, 1981.